The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/01/2014

SUBJECT:

Multiple Security Vulnerabilities Reported in Siemens SIMATIC WinCC

OVERVIEW:

Multiple vulnerabilities have been discovered in the Siemen's Supervisory Control and Data Acquisition (SCADA) system, SIMATIC WinCC, which could allow unauthenticated remote code execution. SIMATIC WinCC is a SCADA system that is used to monitor and control physical processes involved in industry and infrastructure. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical. Successful exploitation of these vulnerabilities could allow an attacker access to sensitive information or allow a user to gain privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

Exploits that target these vulnerabilities are potentially available. Indicators exist that this vulnerability may have been exploited during a recent campaign.

SYSTEM AFFECTED:

- All versions of SIMATIC WinCC prior to version 7.3 Update 2
- All versions of SIMATIC PCS7 (as WinCC is incorporated) prior to version 8.1 Update 2
- All versions of TIA Portal (including WinCC Professional Runtime) prior to V13 Update 6

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in SIMATIC WinCC. Details of these vulnerabilities are as follows:

- An unauthenticated remote attacker could execute arbitrary code via crafted packets [CVE-2014-8551] – A component within WinCC could allow remote code execution for unauthenticated users if specially crafted packets are sent to the WinCC server.
- An unauthenticated remote attacker could read arbitrary files via crafted packets [CVE-2014-8552] - A component within WinCC could allow unauthenticated users to extract arbitrary files from the WinCC server if specially crafted packets are sent to the server.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to SIMATIC WinCC v7.3 Update 2 as these vulnerabilities have been mitigated in this version.
- White list trusted networks and clients.
- Only allow trusted traffic over TCP port 1433.
- Deactivate all unnecessary users on the WinCC server.

REFERENCES:

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8551

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8552

ICS-CERT:

https://ics-cert.us-cert.gov/advisories/ICSA-14-329-02